ON COMPLEXITY OF TRELLIS STRUCTURE OF LINEAR BLOCK CODES

Technical Report

to

NASA

Goddard Space Flight Center

Greenbelt, Maryland 20771

Grant Number NAG 5-931

Report Number NASA 90-004

Shu Lin

Principal Investigator

Department of Electrical Engineering

University of Hawaii at Manoa

Honolulu, Hawaii 96822

October 15, 1990

ON COMPLEXITY OF TRELLIS STRUCTURE OF LINEAR BLOCK CODES[†]

Abstract

This paper is concerned with the trellis structure of linear block codes. The paper consists of four parts. In the first part, we investigate the state and branch complexities of a trellis diagram for a linear block code. A trellis diagram with the minimum number of states is said to be minimal. First, we express the branch complexity of a minimal trellis diagram for a linear block code in terms of the dimensions of specific subcodes of the given code. Then we derive upper and lower bounds on the number of states of a minimal trellis diagram for a linear block code, and show that a cyclic(or shortened cyclic) code is the worst in terms of the state complexity among the linear block codes of the same length and dimension. Furthermore, we show that the structural complexity of a minimal trellis diagram for a linear block code depends on the order of its bit positions. This fact suggests that an appropriate permutation of the bit positions of a code may result in an equivalent code with a much simpler minimal trellis diagram. In part two, we consider boolean polynomial representation of codewords of a linear block code. This representation will help us in study of the trellis structure of the code. In part three, we apply boolean polynomial representation of a code to construct its minimal trellis diagram. Particularly, we focus on the construction of minimal trellises for Reed-Muller codes and the extended and permuted binary primitive BCH codes which contain Reed-Muller code as subcodes. Finally, we analyze and present the structural complexity of minimal trellises for the extended and permuted (64,24), (64,45), and double-error-correcting $(2^m, 2^m - 2m - 1)$ BCH codes. We show that these codes have relatively simple trellis structure and hence can be decoded with the Viterbi decoding algorithm.

1. Introduction

For years, it has been a common belief among the coding theorists that block codes do not have simple trellis structure as convolutional codes do and maximum likelihood decoding of block codes with the Viterbi decoding algorithm is practically impossible, except for very short codes with small dimensions. As a result of this common belief, very little research effort has been expended in the study of trellis structure of block codes. It is really a pity that over the years, there are only four major papers[1–4] touching on the subject of trellis structure of block codes comparing with hundreds of papers dealing with other algebraic and geometric structure and properties of block codes.

This paper is concerned with the trellis structure of linear block codes. We show that some linear block codes of moderate length do have reasonably simple trellises and hence can be decoded with the Viterbi decoding algorithm. Our study is motivated by the works of Wolf [1] and Forney [2, 3], especially Forney's latest work [3] in which he presented a trellis construction for linear block codes and asserted that the construction results in minimal trellises in the sense of number of states.

The presentation of this paper is organized as follows. In Section 2, the branch complexity of the minimal trellis diagram for a linear block code is analyzed, and is expressed in terms of the dimensions of specific linear subcodes of the given code. Upper and lower bounds on the number of states of a minimal trellis diagram for a linear block code are derived. We show that a cyclic (or shortened cyclic) code is the worst in terms of the number of states in its minimal trellis diagram among the linear block codes of the same length and dimension. Furthermore, we show that the complexity of the minimal trellis diagram for a linear block code depends on the order of its bit positions. This fact suggests that an appropriate permutation of the bit positions of a linear block code may result in an equivalent code with a considerably simpler trellis diagram. We are particularly interested in finding appropriate permutations of bit positions of binary primitive BCH codes for reducing the number of states in their trellises. The binary primitive BCH code of length $2^m - 1$ and minimum Hamming distance $2^{m-r} - 1$ contains the cyclic r-th order Reed-Muller code of length $2^m - 1$ as a subcode [5, 6], and the dual code of the even weight subcode of the binary primitive BCH code of length $2^m - 1$ and a specific designed distance, denoted $q(m, r)$, contains the cyclic r-th order Reed-Muller code of length $2^m - 1$ as a subcode for $q(m, r) = 5$, $q(m, 2) = 2^{\lfloor m/2 \rfloor} + 3, \ldots$. It is known that

the state complexity of the minimal trellis diagram for a linear binary block code is the same as that for its dual code [1, 3], and the noncyclic Reed-Muller codes of length 2^m in their original form [5] have relatively simple trellis diagrams [3]. From these facts, we determine a permutation of the bit positions of an extended primitive BCH code of length 2^m which results in an equivalent code with a considerably simpler trellis diagram.

In Section 3, we consider boolean polynomial representation of codewords of a cyclic code. This representation helps us in study of the trellis structure of the code obtained from a cyclic code under a certain permutation of bit positions. In Section 4, we apply boolean polynomial representation of a code to construct its trellis diagram. Particularly, we focus on the construction of minimal trellises for Reed-Muller codes and the extended and permuted primitive BCH codes which contain Reed-Muller codes as subcodes. Finally, we conclude the paper by analyzing the state and branch complexities of minimal trellises for the extended and permuted (64,24), (64,45), and double-error-correcting $(2^m, 2^m - 2m - 1)$ BCH codes. We show that the complexity of trellises for these codes are considerably less than that for the original codes in cyclic form without bit-position permutation. Because of their relatively simple trellis structure, these codes can be practically decodes with the Viterbi decoding algorithm.

2. Structure of a minimal trellis diagram for a linear code

In this section, the structural complexity of a trellis diagram with the minimum number of states for a linear block code is studied. For simplicity, we will consider a binary linear code. The extension to a nonbinary linear code is straightforward.

Let C be a binary block (linear or nonlinear) code of length N. An N-section trellis diagram for C is a modified state diagram of a finite automaton $F[C]$ which accepts the set of all binary N-tuples in C, where a modified state diagram means the diagram obtained from a deterministic or nondeterministic state diagram by deleting every state that is not reachable from the initial state or from which there is no path to the final state. By a trellis diagram, we mean an N-section trellis diagram where N is the code length.

Let T be a trellis diagram for C, and for a nonnegative integer h not greater than N, let S_h denote the set of states of T just after the h-th bit position, where S_0 consists of the initial state s_0 only and S_N consists of the final state s_F only. For two states s and s', let $L(s, s')$

denote the set of all label sequences (paths) from s to s'. Then $L(s_0, s_F) = C$. For a binary N-tuple $\mathbf{v} = (v_1, v_2, \ldots, v_N)$, let $p_{h_1,h_2}\mathbf{v}$ denote the binary $(h_2 - h_1)$-tuple $(v_{h_1+1}, v_{h_1+2}, \ldots, v_{h_2})$ and let $p_{h_1,h_2}[C]$ be defined as

$$p_{h_1,h_2}[C] \triangleq \{p_{h_1,h_2}\mathbf{v} \ : \ \mathbf{v} \in C\}. \tag{2.1}$$

Let $\mathbf{u} = (u_1, u_2, \ldots, u_i)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_j)$ be two binary sequences of lengths i and j respectively. The concatenation of $\mathbf{u}$ and $\mathbf{v}$ is defined as the following sequence of length $i+j$:

$$\mathbf{u} \circ \mathbf{v} \triangleq (u_1, u_2, \ldots, u_i, v_1, v_2, \ldots, v_j).$$

Then the definition of a trellis diagram implies that for $0 \leq h < h' \leq N$,
(1)

$$\bigcup_{s \in S_h} \bigcup_{s' \in S_{h'}} L(s, s') = p_{h,h'}[C], \tag{2.2}$$

and
(2) For $\mathbf{u}_1$ and $\mathbf{u}_2$ in $L(s_0, s)$ with $s \in S_h$ and any binary sequence $\mathbf{v}$ of length $N - h$,

$$\mathbf{u}_1 \circ \mathbf{v} \in C \Longleftrightarrow \mathbf{u}_2 \circ \mathbf{v} \in C. \tag{2.3}$$

Hereafter we assume that C is a linear binary (N, K) code. For two integers h_1 and h_2 such that $0 \leq h_1 < h_2 \leq N$, let C_{h_1,h_2} be the linear subcode of C consisting of all codewords whose components are all zero except for the $h_2 - h_1$ components from the $(h_1 + 1)$-th bit position to the h_2-th bit position. Let $K_{h_1,h_2,C}$ (or K_{h_1,h_2}) be the dimension of C_{h_1,h_2}, i.e.,

$$K_{h_1,h_2} = \log_2 |C_{h_1,h_2}|$$

where for a set S, $|S|$ denotes the number of elements in S. For convenience, $K_{h,h}$ is defined as zero. For simplicity, we write $C^{tr}_{h_1,h_2}$ for $p_{h_1,h_2}[C_{h_1,h_2}]$, the truncation of C_{h_1,h_2}. Clearly, $C^{tr}_{h_1,h_2}$ and C_{h_1,h_2} have the same dimension, and $C^{tr}_{h_1,h_2}$ is a linear subcode of $p_{h_1,h_2}[C]$. Then the condition (2.3) is equivalent to the following condition:

$$\mathbf{u}_1 + \mathbf{u}_2 \in C^{tr}_{0,h}. \tag{2.4}$$

i.e., $\mathbf{u}_1 + \mathbf{u}_2$ is a codeword in $C^{tr}_{0,h}$. For a linear code A and its linear subcode B, let A/B denote the set of cosets in A with respect to B. It follows from (2.2) and (2.4) that for $s \in S_h$,

$L(s_0, s)$ is a subset of a coset in $p_{0,h}[C]/C^{tr}_{0,h}$ and the number of states in S_h is lower bounded by

$$|S_h| \geq |p_{0,h}[C]|/|C^{tr}_{0,h}|. \tag{2.5}$$

Let $C_{\overline{h_1,h_2}}$ denote the linear subcode of C consisting of all codewords whose components from the (h_1+1)-th bit position to the h_2-th bit position are all zero, and let $K_{\overline{h_1,h_2},C}$ (or $K_{\overline{h_1,h_2}}$) denote $\log_2 |C_{\overline{h_1,h_2}}|$, the dimension of $C_{\overline{h_1,h_2}}$. Then it follows from the definitions of C_{h_1,h_2} and $C_{\overline{h_1,h_2}}$ that

$$K_{\overline{0,h}} = K_{h,N}, \tag{2.6}$$

$$K_{\overline{h,N}} = K_{0,h}. \tag{2.7}$$

Note that for $0 \leq h_1 < h_2 \leq N$,

$$|p_{h_1,h_2}[C]| = 2^{K-K_{\overline{h_1,h_2}}}. \tag{2.8}$$

For integers h_1, h_2 and h_3 such that $0 \leq h_1 < h_2 < h_3 \leq N$, let $K_{h_1,h_2,h_3,C}$ (or K_{h_1,h_2,h_3}) be defined as

$$K_{h_1,h_2,h_3} \triangleq K_{h_1,h_3} - K_{h_1,h_2} - K_{h_2,h_3}. \tag{2.9}$$

For simplicity, we write K_h (or $K_{h,C}$) for $K_{0,h,N}$ (or $K_{0,h,N,C}$). From (2.5), (2.6) and (2.8) we see that

$$|S_h| \geq 2^{K-K_{\overline{0,h}}-K_{0,h}} = 2^{K-K_{h,N}-K_{0,h}} = 2^{K_h}. \tag{2.10}$$

If there is a one-to-one correspondence between S_h and $p_{0,h}[C]/C^{tr}_{0,h}$ such that $L(s_0, s)$ is a coset of $p_{0,h}[C]/C^{tr}_{0,h}$, then the equality in (2.10) holds, and for s in S_h and different s'_1 and s'_2 in $S_{h'}$, $L(s, s'_1)$ and $L(s, s'_2)$ have no common sequence. Such a trellis diagram can be obtained from the reduced deterministic state diagram of the finite automaton $F[C]$ with the minimum number of states and is said to be minimal. A minimal trellis diagram is unique within graph isomorphism and the number of states in S_h, $|S_h|$, is given by

$$|S_h| = 2^{K_h}. \tag{2.11}$$

This was first given by Forney [3, Appendix A].

Let T be the minimal trellis diagram for a linear binary (N, K) code C. For a state s of T, let $\varphi(s)$ denote the coset leader of the coset corresponding to the state s. Now we will

show how to find $L(s,s')$ for two states s and s' of T. Let h and h' be integers such that $0 \le h < h' \le N$. From the definition of φ, it follows that for $s \in S_h$ and $s' \in S_{h'}$,

$$L(s_0,s) = \{\varphi(s)\} + C^{tr}_{0,h}, \tag{2.12}$$

$$L(s_0,s') = \{\varphi(s')\} + C^{tr}_{0,h'}, \tag{2.13}$$

where for two codes A and B of the same code length, $A+B \triangleq \{\mathbf{u}+\mathbf{v} : \mathbf{u} \in A \text{ and } \mathbf{v} \in B\}$. For $s \in S_h$, $s' \in S_{h'}$ and a binary sequence $\mathbf{v}$ of length $h'-h$, $\mathbf{v} \in L(s,s')$ if and only if

$$L(s_0,s) \circ \{\mathbf{v}\} \subseteq L(s_0,s'), \tag{2.14}$$

where $A \circ B \triangleq \{\alpha \circ \beta : \alpha \in A \text{ and } \beta \in B\}$ for two sets A and B of binary sequences. If $\mathbf{u}$ and $\mathbf{u}'$ are in $L(s_0,s)$, and $\mathbf{u} \circ \mathbf{v}$ and $\mathbf{u}' \circ \mathbf{v}'$ are in $L(s_0,s')$, then it follows from (2.12) and (2.13) that

$$\mathbf{u}+\mathbf{u}' \in C^{tr}_{0,h}, \tag{2.15}$$

$$(\mathbf{u}+\mathbf{u}') \circ (\mathbf{v}+\mathbf{v}') \in C^{tr}_{0,h'}. \tag{2.16}$$

From (2.15), $(\mathbf{u}+\mathbf{u}') \circ 0^{h'-h} \in C^{tr}_{0,h'}$, where $0^{h'-h}$ denotes a sequence of $h'-h$ zeros, and from (2.16) it follows that $0^h \circ (\mathbf{v}+\mathbf{v}') \in C^{tr}_{0,h'}$. Clearly,

$$\mathbf{v}+\mathbf{v}' \in C^{tr}_{h,h'}. \tag{2.17}$$

Note that $C^{tr}_{0,h} \circ C^{tr}_{h,h'}$ is a linear subcode of $C^{tr}_{0,h'}$. Let $\{\alpha_i \circ \beta_i : |\alpha_i|_\ell = h, |\beta_i|_\ell = h'-h, 1 \le i \le 2^{K_{0,h,h'}}\}$ be the set of all coset leaders of $C^{tr}_{0,h'}/(C^{tr}_{0,h} \circ C^{tr}_{h,h'})$, where $|\alpha|_\ell$ denotes the length of binary sequence α. For two different coset leaders $\alpha_i \circ \beta_i$ and $\alpha_{i'} \circ \beta_{i'}$ with $1 \le i < i' \le 2^{K_{0,h,h'}}$,

$$\alpha_i \ne \alpha_{i'} \text{ and } \beta_i \ne \beta_{i'}. \tag{2.18}$$

Each β_i is said to be corresponding to α_i. (Assume the contrary, e.g. $\alpha_i = \alpha_{i'}$. Then $\alpha_i \circ \beta_i + \alpha_i \circ \beta_{i'} = 0^h \circ (\beta_i + \beta_{i'}) \in C^{tr}_{0,h'}$, which implies that $\beta_i + \beta_{i'} \in C^{tr}_{h,h'}$, that is, $\alpha_i \circ \beta_i$ and $\alpha_{i'} \circ \beta_{i'}$ are in the same coset of $C^{tr}_{0,h'}/(C^{tr}_{0,h} \circ C^{tr}_{h,h'})$, a contradiction.) Hence we see that

$$p_{0,h}[C_{0,h'}]/C^{tr}_{0,h} \leftrightarrow \{\alpha_i : 1 \le i \le 2^{K_{0,h,h'}}\} \tag{2.19}$$

$$p_{h,h'}[C_{0,h'}]/C^{tr}_{h,h'} \leftrightarrow \{\beta_i : 1 \le i \le 2^{K_{0,h,h'}}\} \tag{2.20}$$

where "$A \leftrightarrow B$" means that B can be chosen as the set of all coset leaders of A.

Lemma 1: For $0 \leq h < h' \leq N$, let $s \in S_h$ and $s' \in S_{h'}$. Let $\varphi(s')$ be represented as

$$\varphi(s') = \alpha \circ \beta, \tag{2.21}$$

where $|\alpha|_\ell = h$ and $|\beta|_\ell = h' - h$.

(1) If there is a positive integer i not greater than $2^{K_{0,h,h'}}$ such that

$$\varphi(s) = \alpha + \alpha_i \pmod{C^{tr}_{0,h}}, \tag{2.22}$$

then $L(s, s')$ is given as

$$L(s, s') = \{\beta + \beta_i\} + C^{tr}_{h,h'}. \tag{2.23}$$

(2) Otherwise, $L(s, s')$ is empty.

Proof: Suppose that $L(s, s')$ is not empty. It follows from (2.13), (2.14), (2.19) and (2.21) that

$$\begin{aligned} L(s_0, s) &\subseteq \{\alpha\} + p_{0,h}[C^{tr}_{0,h'}] \\ &\subseteq \{\alpha\} + \{\alpha_i : 1 \leq i \leq 2^{K_{0,h,h'}}\} + C^{tr}_{0,h}. \end{aligned} \tag{2.24}$$

From (2.12) and (2.24), we have that

$$\varphi(s) \in \{\alpha + \alpha_i \ : \ 1 \leq i \leq 2^{K_{0,h,h'}}\} + C^{tr}_{0,h}.$$

That is, there exists α_i which satisfies (2.22). Conversely, suppose that such an α_i exists. Then it holds that for any $\gamma \in C^{tr}_{0,h}$,

$$\begin{aligned} (\alpha + \alpha_i + \gamma) \circ (\beta + \beta_i) &= (\alpha \circ \beta) + (\alpha_i \circ \beta_i) + (\gamma \circ 0^{h'-h}) \\ &\in \{\varphi(s')\} + C^{tr}_{0,h'} + (C^{tr}_{0,h} \circ C^{tr}_{h,h'}) \\ &\in \{\varphi(s')\} + C^{tr}_{0,h'} \\ &\in L(s_0, s'). \end{aligned} \tag{2.25}$$

From (2.14) and (2.25), we see that $\beta + \beta_i \in L(s, s')$. Then the equality (2.23) follows from (2.17). $\Delta\Delta$

This lemma says that $L(s, s')$ is either empty or a coset of $p_{h,h'}[C]/C^{tr}_{h,h'}$. From this lemma, we have Theorem 1 (refer to Figure 1) which describes the structure of the minimal trellis diagram for a linear block code.

Theorem 1: For $1 \leq h \leq N$, let S_h be the set of states of the minimal trellis diagram for a linear binary (N, K) code. For $1 \leq h < h' \leq N$, S_h and $S_{h'}$ can be partitioned into 2^q blocks of the same size $S_{h1}, S_{h2}, \ldots, S_{h2^q}$ and $S_{h'1}, S_{h'2}, \ldots, S_{h'2^q}$, respectively, where $q \triangleq K_{0,h,N} - K_{0,h,h'}$, in such a way that (1) there is a path from $s \in S_h$ to $s' \in S_{h'}$, if and only if $s \in S_{hi}$ and $s' \in S_{h'i}$ for the same i, (2) for $s \in S_{hi}$ and $s' \in S_{h'i}$ with $1 \leq i \leq 2^q$, $L(s, s')$ is a coset of $p_{h,h'}[C]/C^{tr}_{h,h'}$ and (3) the number of paths from s to s' is $2^{K_{h,h'}}$.

Proof: See Appendix A. ΔΔ

Now we consider the complexity of the minimal trellis diagram for the dual code $C^\perp$ of C. It can be easily proved that for $0 \leq h < h' \leq N$, $C^{tr}_{h,h'}$ and $p_{h,h'}[C^\perp]$ are duals (Lemma 6 in [3, Appendix A] is for $h = 0$). Hence it follows from (2.8) that

$$K_{h,h',C^\perp} = h' - h - K + K_{\overline{h,h'},C}. \tag{2.26}$$

From (2.6), (2.7), (2.9) and (2.26), the following identities hold:

$$K_{h,C} = K_{h,C^\perp}, \tag{2.27}$$

$$K_{0,h,N,C^\perp} - K_{0,h,h',C^\perp} = K_{\overline{h,h'},C} - K_{0,h,C} - K_{h',N,C}. \tag{2.28}$$

Identity (2.27) was given in [3, Corollary, Appendix A]. The equality of (2.27) actually says that the minimal trellis diagrams for a linear block code and its dual have the same state complexity.

Next we show a condition for a code to be the worst in terms of the number of states of its trellis diagram. Since $K_{0,h} \geq K - N + h$ and $K_{h,N} \geq K - h$,

$$K_h \leq \min(h, N - h). \tag{2.29}$$

It is also known [1] that

$$K_h \leq \min(K, N - K). \tag{2.30}$$

Consequently, it holds that

$$K_h \leq \min(h, N - h, K, N - K). \tag{2.31}$$

Lemma 2: If C has a generator matrix (or a parity-check matrix) of which the first K (or $N - K$) columns and the last K (or $N - K$) columns are linearly independent respectively, then the equality in (2.31) holds for $0 \leq h \leq N$.

Proof: The assumption on a generator matrix implies that

$$K_{0,h} = \max(0, K - N + h), \tag{2.32}$$

$$K_{h,N} = \max(0, K - h). \tag{2.33}$$

Then we have that

$$\begin{aligned} K_h &= K - \max(0, K - N + h) - \max(0, K - h) \\ &= \min(K, N - h) - \max(0, K - h) \\ &= \min(K, N - h, h, N - K). \end{aligned} \tag{2.34}$$

$\Delta\Delta$

If the condition of Lemma 2 holds for a parity-check matrix, consider the dual code.

Then Lemma 2 follows form (2.27) and (2.34). The inverse of the above lemma also holds. If C is a cyclic or shortened cyclic code, then any K consecutive columns of a generator matrix of C are linearly independent, and therefore, the equality in (2.31) holds for $0 \leq h \leq N$. In order to obtain a trellis diagram with a smaller number of states for a cyclic or shortened cyclic code, the order of bit positions must be permuted. For a permutation π on $1, 2, \ldots, N$ and an N-tuple $\mathbf{v} = (v_1, v_2, \ldots, v_N)$, let $\pi\mathbf{v}$ denote $(v_{\pi(1)}, v_{\pi(2)}, \ldots, v_{\pi(N)})$ and for a code C of length N, let $\pi[C]$ be defined as

$$\pi[C] \triangleq \{\pi\mathbf{v} \ : \ \mathbf{v} \in C\}. \tag{2.35}$$

Lemma 3 can be used for finding a proper permutation to reduce the state complexity of the minimal trellis diagram for a cyclic or shortened cyclic code.

Lemma 3: Let C' be a linear $(N, K - k)$ subcode of C or a linear $(N, N - K - k)$ subcode of the dual code $C^{\perp}$ of C. For a permutation π on $1, 2, \ldots, N$,

$$K_{h,\pi[C]} \leq K_{h,\pi[C']} + k. \tag{2.36}$$

Proof: First consider the case where C' is a subcode of C. Since $K_{0,h,\pi[C]} \geq K_{0,h,\pi[C']}$ and $K_{h,N,\pi[C]} \geq K_{h,N,\pi[C']}$, inequality (2.36) follows from the definition of K_h. For the case where C' is a subcode of $C^{\perp}$, this lemma follows form (2.27) and (2.36) for $C^{\perp}$. $\Delta\Delta$

Let ex-C denote the extended code obtained from C by adding an overall parity bit to each codeword in C. Let $\mathrm{BCH}_{m,d}$ denote the binary primitive (or narrow-sense) BCH code of length $2^m - 1$ and designed distance d. Let c-$\mathrm{RM}_{m,r}$ denote the cyclic r-th order Reed-Muller code of length $2^m - 1$ [5, 6]. It is known that c-$\mathrm{RM}_{m,r}$ is a subcode of the $\mathrm{BCH}_{h,2^{m-r}-1}$.

Example 1: For $1 \leq r < m$, let C and C' be ex-$\mathrm{BCH}_{m,2^{m-r}-1}$ and ex-c-$\mathrm{RM}_{m,r}$ respectively. Then C' is a subcode of C. There is a permutation π on the bit positions (see section 4) such that $\pi[C'] = \mathrm{RM}_{m,r}$, the r-th order (noncyclic) Reed-Muller code of length 2^m [5, 7]. Let $T_1, T_2, \ldots, T_M$ be trellis diagrams for the cosets of $\pi[C]/\pi[C']$, respectively, where $M = |C/C'|$. These trellis diagrams are isomorphic to each other except for branch labels. A (nondeterministic in general) trellis diagram for $\pi[C]$ with M parallel subdiagrams is obtained from $T_1, T_2, \ldots, T_M$ by merging the initial states and the final states of $T_1, T_2, \ldots, T_M$ into a single initial state and a single final state, respectively. It is known that r-th order noncyclic Reed-Muller code $\mathrm{RM}_{m,r}$ has a relatively simple diagram [3]. This fact suggests that for small M, the code $\pi[\text{ex-}\mathrm{BCH}_{m,2^{m-r}-1}]$ also has a relative simple trellis diagram. $\Delta\Delta$

Let $h_0, h_1, h_2, \ldots, h_m$ be integers such that

$$h_0 = 0 < h_1 < h_2 < \ldots < h_{m-1} < h_m = N.$$

An m-section trellis diagram for C can be obtained from the minimal trellis diagram T by deleting every state in S_h for $h \in \{0, 1, \ldots, N\} - \{h_0, h_1, \ldots, h_m\}$ and every branch to or from a deleted state and by writing a branch with label α from a state $s \in S_{h_i}$ to a state $s' \in S_{h_{i+1}}$ for $0 \leq i < m$, if and only if there is a path with label α from s to s' in T. This m-section trellis diagram is said to be minimal, and if $h_{i+1} - h_i$ is the same for $0 \leq i < m$, it is said to have the same section length.

If the binary code of length $N\ell$ derived from a 2^ℓ-ary PSK or QASK block modulation code C of length N by representing each symbol as a binary sequence uniquely is linear under the modulo-2 addition [8], then the method described in this section can be applied to construct a trellis diagram for C.

3. Boolean polynomial representation of a cyclic code

In this section, we consider boolean polynomial representation of a cyclic code. We show that the codewords of a binary cyclic code of length $2^m - 1$ (or its extended code) can be expressed by boolean polynomials with m variables. A method for finding the polynomial representation of a basis of any cyclic subcode of the given cyclic code is presented. This boolean polynomial representation is very useful in study of the trellis structure of the code or its equivalent code obtained by permuting its bit positions under a certain permutation.

Let α be a primitive element of the Galois field GF(2^m), and let $\beta_1, \beta_2, \ldots, \beta_m$ be a basis of GF(2^m) over GF(2). For a positive integer i less than 2^m, let α^{i-1} be expressed as

$$\alpha^{i-1} = \sum_{j=1}^{m} a_{ij}\beta_j, \tag{3.1}$$

with $a_{ij} \in$ GF(2). For $i = 0$, let $a_{0j} \triangleq 0$ for $1 \leq j \leq m$. Let n denote $2^m - 1$ in this section. For a binary n-tuple $\bar{v} = (v_1, v_2, \ldots, v_n)$, a boolean polynomial with m variables, $f(x_1, x_2, \ldots, x_m)$, is said to represent $\bar{v}$ (with respect to a cyclic order of bit positions) if and only if for $1 \leq i \leq n$,

$$v_i = f(a_{i1}, a_{i2}, \ldots, a_{im}), \tag{3.2}$$

where $(a_{i1}, a_{i2}, \ldots, a_{im})$ is the binary representation of α^{i-1} with respect to $\beta_1, \beta_2, \ldots, \beta_m$. A boolean polynomial $f(x_1, x_2, \ldots, x_m)$ is also said to represent a binary $n+1$-tuple,

$$\bar{v}_{\text{ex}} = (v_0, v_1, \ldots, v_n),$$

if and only if $v_0 = f(0, 0, \ldots, 0)$ and the equality (3.2) holds for $1 \leq i \leq n$. If a boolean polynomial f of degree $m-1$ or less represents a binary n-tuple $(v_1, v_2, \ldots, v_n)$, then f also represents the $(n+1)$-tuple $(\sum_{i=1}^{n} v_i, v_1, v_2, \ldots, v_n)$. For a boolean polynomial f, let $c(f)$ denote the binary n-tuple (or $(n+1)$-tuple) represented by f with respect to a cyclic order of bit positions.

For $0 \leq i \leq n$, represent i in the standard binary form as $i = \sum_{j=1}^{m} i_j 2^{j-1}$. Then the binary weight of i, denoted $w(i)$, is defined as the number of nonzero i_j's. If follows from the definition that

$$w(n-i) = m - w(i). \tag{3.3}$$

Let I_m denote the set of the cyclotomic coset representatives mod $2^m - 1$, and for $i \in I_m$, let m_i denote the number of integers in the cyclotomic coset whose representative is i. For

$1 \leq j \leq m$, let $T_j(x)$ be defined as

$$T_j(x) \triangleq x + x^2 + x^{2^2} + \cdots + x^{2^{j-1}}. \tag{3.4}$$

Since m_i is a factor of m, GF(2^{m_i}) is a subfield of GF(2^m). For $i \in I_m$, let $\gamma_1^{(m_i)}, \gamma_2^{(m_i)}, \ldots, \gamma_{m_i}^{(m_i)}$ be a basis of GF(2^{m_i}) and for $1 \leq h \leq m_i$, let $f_{i,h}(x_1, x_2, \ldots, x_m)$ be defined as a boolean polynomial of m variables:

$$f_{i,h}(x_1, x_2, \ldots, x_m) \triangleq T_{m_i}(\gamma_h^{(m_i)}(\sum_{j=1}^{m} \beta_j x_j)^{n-i}). \tag{3.5}$$

From (3.3), $n - i$ is expressed as $2^{i_1} + 2^{i_2} + \cdots + 2^{i_\nu}$, where $0 \leq i_1 < i_2 < \cdots < i_\nu < m$ and $\nu = m - w(i)$. Then we have that

$$\begin{aligned} \left(\sum_{j=1}^{m} \beta_j x_j\right)^{n-i} &= \left(\sum_{j=1}^{m} \beta_j x_j\right)^{\sum_{\ell=1}^{\nu} 2^{i_\ell}} \\ &= \prod_{\ell=1}^{\nu} \left(\sum_{j=1}^{m} \beta_j^{2^{i_\ell}} x_j\right). \end{aligned} \tag{3.6}$$

Hence, $f_{i,h}$ is a boolean polynomial of degree $m - w(i)$ or less. In particular, the coefficient of $x_{j_1}, x_{j_2}, \ldots, x_{j_\nu}$ of degree $m - w(i)$ is given by

$$T_{m_i}(\gamma_h^{(m_i)} B_{j_1, j_2, \ldots, j_\nu}) \tag{3.7}$$

where

$$B_{j_1, j_2, \ldots, j_\nu} = \det \begin{pmatrix} \beta_{j_1}^{2^{i_1}} & \beta_{j_1}^{2^{i_2}} & \cdots & \beta_{j_1}^{2^{i_\nu}} \\ \beta_{j_2}^{2^{i_1}} & \beta_{j_2}^{2^{i_2}} & \cdots & \beta_{j_2}^{2^{i_\nu}} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{j_\nu}^{2^{i_1}} & \beta_{j_\nu}^{2^{i_2}} & \cdots & \beta_{j_\nu}^{2^{i_\nu}} \end{pmatrix}. \tag{3.8}$$

For $i \in I_m$, let $g_i(x)$ denote the minimum polynomial of α^i. Theorem 2 follows from (3.1), (3.2), (3.5) and the property of Mattson-Solomon polynomial [5, 7].

Theorem 2: Let C be a binary cyclic (n, k) code with generator polynomial $\prod_{i \in I} g_i(x)$ where $I \subset I_m$. Let $P_B(C)$ be defined as

$$P_B(C) \triangleq \{f_{i,h} : i \in I_m - I \text{ and } 1 \leq h \leq m_i\}. \tag{3.9}$$

There is a one-to-one correspondence between $P_B(C)$ and a basis B of C such that each polynomial in $P_B(C)$ represents a codeword in B. $\Delta\Delta$

Let C' be a cyclic (n, k') subcode of C with generator polynomial $\prod_{i\in I'} g_i(x)$ where $I \subset I' \subset I_m$. We partition C into $2^{k-k'}$ cosets with respect to C'. As the set of coset leaders, we choose a cyclic $(n, k-k')$ subcode with generator polynomial $\prod_{i\in I\cup(I_m-I')} g_i(x)$. Let this subcode be denoted $C - C'$. Then it follows from the Theorem 2 that there is a one-to-one correspondence between a basis of the set of $2^{k-k'}$ coset leaders and the following set of boolean polynomials:

$$P_B(C - C') \triangleq \{f_{i,h} : i \in I' - I \text{ and } 1 \le h \le m_i\}. \tag{3.10}$$

Therefore, C is uniquely specified by $P_B(C')$ and $P_B(C - C')$.

Consider a special case where $m_i < m$. Then $i = 1 + 2^{m_i} + 2^{2m_i} + \cdots + 2^{m-m_i}$, and $w(i) = m/m_i$. Then

$$n - i = \sum_{t=1}^{m_i-1} \sum_{s=1}^{w(i)} 2^{t+m_i(s-1)}. \tag{3.11}$$

Let $\{\gamma_1, \gamma_2, \ldots, \gamma_{m_i}\}$ be a basis of GF(2^{m_i}) over GF(2), and let $\{\delta_1, \delta_2, \ldots, \delta_{w(i)}\}$ be a basis of GF(2^m) over GF(2^{m_i}). For $1 \le j \le m_i$ and $1 \le h \le w(i)$, let $\beta_{j+m_i(h-1)}$ be defined as

$$\beta_{j+m_i(h-1)} \triangleq \gamma_j \delta_h. \tag{3.12}$$

Then $\beta_1, \beta_2, \ldots, \beta_m$ is a basis of GF(2^m) over GF(2). For $1 \le j \le m_i$, $1 \le t \le m_i$, $1 \le h \le w(i)$ and $1 \le s \le w(i)$,

$$\beta_{j+m_i(h-1)}^{2^{t+m_i(s-1)}} = \gamma_j^{2^t} \delta_h^{2^{t+m_i(s-1)}}. \tag{3.13}$$

This is used in the following Examples 2 and 3.

Example 2: Let C be $\text{BCH}_{6,15}$, the binary primitive (63,24) BCH code with minimum distance 15 and C' be c-$\text{RM}_{6,2}$, the cyclic (62,22) 2nd order Reed-Muller code [5]. Then C' is a subcode of C and consists of the set of all binary n-tuples represented by boolean polynomials of degree 2 or less [7]. Then $I' - I$ in (3.10) consists of $21 (= 1 + 2^2 + 2^4)$ only, and $w(21) = 3$, $\nu = m - w(21) = 3$, $m_{21} = 2$ and $n - 21 = 2 + 2^3 + 2^5$. It follows from (3.10) that $f_{21,1}^{(3)}$ and $f_{21,2}^{(3)}$ represent two codewords in C which form a basis of the coset leaders of C/C', where $f^{(j)}$ denotes the polynomial consisting of the terms of degree j in f. Suppose that $\{\gamma_1, \gamma_2\}$ is a basis of GF(2^2) over GF(2), and $\{\delta_1, \delta_2, \delta_3\}$ is a basis of GF(2^6) over GF(2^2). Let $\beta_1, \beta_2, \ldots, \beta_6$ be defined as (3.12). Now consider B_{j_1,j_2,j_3} given by (3.8) with different j_1, j_2 and j_3 in $\{1, 2, \ldots, 6\}$. It follows from (3.8), (3.11) to (3.13) that (i) if there are j and j' in

$\{j_1, j_2, j_3\}$ such that $j' = j + 1$ and j is odd, then

$$(\beta_{j'}^2, \beta_{j'}^{2^3}, \beta_{j'}^{2^5}) = \gamma_2^2 \gamma_1^{-2} (\beta_j^2, \beta_j^{2^3}, \beta_j^{2^5})$$

and therefore,

$$B_{j_1,j_2,j_3} = 0, \tag{3.14}$$

and (ii) otherwise, for a binary 3-tuple (a_1, a_2, a_3),

$$B_{1+a_1,3+a_2,5+a_3} = (\gamma_2^2 \gamma_1^{-2})^{a_1+a_2+a_3} B_{1,3,5}. \tag{3.15}$$

Here $B_{1,3,5} \in \mathrm{GF}(2^2) - \{0\}$ [7, p.117, Lemma 18]. We can choose $\delta_1, \delta_2, \delta_3$ to make $B_{1,3,5}$ to be one. Without loss of generality, take 1 for γ_1 and a primitive element γ for γ_2, then

$$B_{1+a_1,3+a_2,5+a_3} = 1, \quad \text{if } a_1 + a_2 + a_3 \equiv 0 \pmod 3, \tag{3.16}$$

$$= \gamma, \quad \text{if } a_1 + a_2 + a_3 \equiv 2 \pmod 3, \tag{3.17}$$

$$= 1 + \gamma, \quad \text{if } a_1 + a_2 + a_3 \equiv 1 \pmod 3. \tag{3.18}$$

In (3.1), let $\gamma_1^{(2)} \triangleq 1$ and $\gamma_2^{(2)} \triangleq \gamma$. Then it follows from (3.5), (3.7), (3.8) and (3.16) to (3.18) that

$$f_{21,1}^{(3)} = x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_5, \tag{3.19}$$

$$f_{21,2}^{(3)} = x_1x_3x_5 \oplus x_1x_4x_6 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_6. \tag{3.20}$$

Summarizing the above results, we see that C is the union of four cosets with respect to C' whose leaders are generated by $c(f_{21,1}^{(3)})$ and $c(f_{21,2}^{(3)})$.

Let T_1 be a trellis diagram for C'. Then the other three cosets of C/C' would have trellis diagrams, T_2, T_3 and T_4, isomorphic to T_1. As a result, C has a trellis diagram which consists of 4 parallel isomorphic subdiagrams without cross connections among them. The state complexity of the overall trellis diagram can be greatly reduced if a proper bit position permutation is performed on C and C' (this is shown in Section 4). $\Delta\Delta$

Example 3: Let C be $\mathrm{BCH}_{6,7}$, the binary primitive $(63, 45)$ BCH code with minimum distance 7 and C' be c-$\mathrm{RM}_{6,3}$, the cyclic $(63, 42)$ 3rd order Reed-Muller code [5]. Then C' is a subcode of C and consists of the set of all binary n-tuples represented by boolean polynomials of degree 3 or less [7]. Note that $I' - I$ in (3.10) consists of $9 (= 1 + 2^3)$ only and $w(9) = 2$,

$\nu = m - w(9) = 4$, $m_9 = 3$ and $n - 9 = 2 + 2^2 + 2^4 + 2^5$. It follows from (3.10) that $f_{9,1}^{(4)}$, $f_{9,2}^{(4)}$ and $f_{9,3}^{(4)}$ represent three codewords in C which from a basis of the coset leaders of C/C', where $f^{(4)}$ denotes the sum of terms of degree 4 in f. Suppose that $\{\gamma_1, \gamma_2, \gamma_3\}$ is a basis of GF(2^3) over GF(2) and $\{\delta_1, \delta_2\}$ is a basis of GF(2^6) over GF(2^3). Note that $\gamma_j^2 = \gamma_j^{2^4}$ and $\gamma_j^{2^2} = \gamma_j^{2^5}$ for $1 \le j \le 3$. Let $\beta_1, \beta_2, \ldots, \beta_6$ be defined as (3.12). Now consider B_{j_1,j_2,j_3,j_4} with $1 \le j_1 < j_2 < j_3 < j_4 \le 6$. There are two cases to be considered:

(i) Suppose that either $j_1 = 1$, $j_2 = 2$ and $j_3 = 3$ or $j_2 = 4$, $j_3 = 5$ and $j_4 = 6$. For $4 \le j \le 6$,

$$\begin{aligned} B_{1,2,3,j} &= \det \begin{pmatrix} \gamma_1^2\delta_1^2 & \gamma_1^{2^2}\delta_1^{2^2} & \gamma_1^2\delta_1^{2^4} & \gamma_1^{2^2}\delta_1^{2^5} \\ \gamma_2^2\delta_1^2 & \gamma_2^{2^2}\delta_1^{2^2} & \gamma_2^2\delta_1^{2^4} & \gamma_2^{2^2}\delta_1^{2^5} \\ \gamma_3^2\delta_1^2 & \gamma_3^{2^2}\delta_1^{2^2} & \gamma_3^2\delta_1^{2^4} & \gamma_3^{2^2}\delta_1^{2^5} \\ \beta_j^2 & \beta_j^{2^2} & \beta_j^{2^4} & \beta_j^{2^5} \end{pmatrix} \\ &= \det \begin{pmatrix} \gamma_1^2\delta_1^2 & \gamma_1^{2^2}\delta_1^{2^2} & 0 & 0 \\ \gamma_2^2\delta_1^2 & \gamma_2^{2^2}\delta_1^{2^2} & 0 & 0 \\ \gamma_3^2\delta_1^2 & \gamma_3^{2^2}\delta_1^{2^2} & 0 & 0 \\ \beta_j^2 & \beta_j^{2^2} & \beta_j^{2^4} + \delta_1^{2^4-2}\beta_j^2 & \beta_j^{2^5} + \delta_1^{2^5-2^2}\beta_j^{2^2} \end{pmatrix} \\ &= 0. \end{aligned} \tag{3.21}$$

Similarly, we have that

$$B_{j,4,5,6} = 0, \quad \text{for } 1 \le j \le 3. \tag{3.22}$$

(ii) Suppose that $1 \le j_1 < j_2 \le 3 < j_3 < j_4 \le 6$. Let j_1' and j_2' be defined as

$$\begin{aligned} j_1' &= j_3 - 3, \\ j_2' &= j_4 - 3. \end{aligned}$$

Then we have that

$$B_{j_1,j_2,j_3,j_4} = \det \begin{pmatrix} \gamma_{j_1}^2\delta_1^2 & \gamma_{j_1}^{2^2}\delta_1^{2^2} & \gamma_{j_1}^2\delta_1^{2^4} & \gamma_{j_1}^{2^2}\delta_1^{2^5} \\ \gamma_{j_2}^2\delta_1^2 & \gamma_{j_2}^{2^2}\delta_1^{2^2} & \gamma_{j_2}^2\delta_1^{2^4} & \gamma_{j_2}^{2^2}\delta_1^{2^5} \\ \gamma_{j_1'}^2\delta_2^2 & \gamma_{j_1'}^{2^2}\delta_2^{2^2} & \gamma_{j_1'}^2\delta_2^{2^4} & \gamma_{j_1'}^{2^2}\delta_2^{2^5} \\ \gamma_{j_2'}^2\delta_2^2 & \gamma_{j_2'}^{2^2}\delta_2^{2^2} & \gamma_{j_2'}^2\delta_2^{2^4} & \gamma_{j_2'}^{2^2}\delta_2^{2^5} \end{pmatrix}$$

$$= \det \begin{pmatrix} \gamma_{j_1}^2\delta_1^2 & \gamma_{j_1}^{2^2}\delta_1^{2^2} & 0 & 0 \\ \gamma_{j_2}^2\delta_1^2 & \gamma_{j_2}^{2^2}\delta_1^{2^2} & 0 & 0 \\ \gamma_{j_1'}^2\delta_1^2 & \gamma_{j_1'}^{2^2}\delta_1^{2^2} & \gamma_{j_1'}^2(\delta_2^{2^4}+\delta_2^2\delta_1^{2^4-2}) & \gamma_{j_1'}^{2^2}(\delta_2^{2^5}+\delta_2^{2^2}\delta_1^{2^5-2^2}) \\ \gamma_{j_2'}^2\delta_1^2 & \gamma_{j_2'}^{2^2}\delta_1^{2^2} & \gamma_{j_2'}^2(\delta_2^{2^4}+\delta_2^2\delta_1^{2^4-2}) & \gamma_{j_2'}^{2^2}(\delta_2^{2^5}+\delta_2^{2^2}\delta_1^{2^5-2^2}) \end{pmatrix}$$

$$= \gamma_{j_1}^2\gamma_{j_2}^2(\gamma_{j_1}^2+\gamma_{j_2}^2)\gamma_{j_1'}^2\gamma_{j_2'}^2(\gamma_{j_1'}^2+\gamma_{j_2'}^2)\delta_1^6\delta_2^6(\delta_1^7+\delta_2^7)^6. \tag{3.23}$$

Note that $\delta_1\delta_2(\delta_1^7+\delta_2^7)$, denoted τ, is in $\mathrm{GF}(2^3)-\{0\}$. Let δ_1' and δ_2' be defined as

$$\begin{aligned} \delta_1' &\triangleq \delta_1, \\ \delta_2' &\triangleq \tau^{-1}\delta_2. \end{aligned}$$

If $\{\delta_1', \delta_2'\}$ is used as a basis of $\mathrm{GF}(2^6)$ over $\mathrm{GF}(2^3)$ in place of $\{\delta_1, \delta_2\}$, then

$$\delta_1'^6\delta_2'^6(\delta_1'^7+\delta_2'^7)^6 = 1. \tag{3.24}$$

Without loss of generality, $\{1, \gamma, \gamma^2\}$ can be chosen as a basis of $\mathrm{GF}(2^3)$ over $\mathrm{GF}(2)$, where γ is a root of x^3+x+1. Then it follows from (3.23) and (3.24) that the sum $f^{(4)}$ of terms of degree 4 in $\left(\sum_{t=1}^{6}\beta_t x_t\right)^{2+2^2+2^4+2^5}$ is given by

$$\begin{aligned} f^{(4)} &= (\gamma x_1x_2 \oplus \gamma^2 x_1x_3 \oplus x_2x_3)(\gamma x_4x_5 \oplus \gamma^2 x_4x_6 \oplus x_5x_6) \\ &= \gamma^2 x_1x_2x_4x_5 \oplus \gamma^3 x_1x_2x_4x_6 \oplus \gamma x_1x_2x_5x_6 \\ &\quad \oplus\gamma^3 x_1x_3x_4x_5 \oplus \gamma^4 x_1x_3x_4x_6 \oplus \gamma^2 x_1x_3x_5x_6 \\ &\quad \oplus\gamma x_2x_3x_4x_5 \oplus \gamma^2 x_2x_3x_4x_6 \oplus x_2x_3x_5x_6. \end{aligned} \tag{3.25}$$

In (3.5), let $\{\gamma_1^{(3)}, \gamma_2^{(3)}, \gamma_3^{(3)}\}$ be the dual basis of $\{1, \gamma, \gamma^2\}$. It follows from (3.5), (3.7), (3.8) and (3.25) that

$$f_{9,1}^{(4)} = x_1x_2x_4x_6 \oplus x_1x_3x_4x_5 \oplus x_2x_3x_5x_6, \tag{3.26}$$

$$f_{9,2}^{(4)} = x_1x_2x_4x_5 \oplus x_1x_3x_4x_6 \oplus x_1x_3x_5x_6 \oplus x_2x_3x_4x_6, \tag{3.27}$$

$$f_{9,3}^{(4)} = x_1x_2x_4x_6 \oplus x_1x_2x_5x_6 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_6 \oplus x_2x_3x_4x_5. \tag{3.28}$$

Summarizing the above results, we conclude that $\mathrm{BCH}_{6,7}$ is the union of eight cosets with respect to c-$\mathrm{RM}_{6,3}$ whose leaders are spanned by the vectors, $c(f_{9,1}^{(4)})$, $c(f_{9,2}^{(4)})$ and $c(f_{9,3}^{(4)})$.

It follows from Example 1 that $\mathrm{BCH}_{6,7}$ (or its equivalent code obtained by permuting its bit position under a certain permutation) has a trellis diagram consisting of 8 parallel isomorphic subdiagrams without cross connections among them. $\Delta\Delta$

Example 4: Let C be the dual code of the even weight subcode of the primitive binary BCH code of length $2^m - 1$ and minimum distance 5, where $m \geq 3$, and C' be the cyclic first order Reed-Muller code of length $2^m - 1$ whose codewords are represented by linear boolean polynomials [7]. Then C' is a subcode of C, and $I' - I$ in (3.10) consists of $\ell = n - 2^{m-2} - 2^{m-1}$, only, and $w(\ell) = m - 2$, $\nu = 2$, $m_\ell = m$ and $n - \ell = 2^{m-2} + 2^{m-1}$. It follows from (3.10) that $f^{(2)}_{\ell,h}$ with $1 \leq h \leq m$ represent m codewords in C which form a basis of $C - C'$, the set of the coset leaders of C/C'. Let $\beta_1, \beta_2, \ldots, \beta_m$ be a basis of $\mathrm{GF}(2^m)$. Then it follows from (3.8) that for $1 \leq j_1 < j_2 \leq m$,

$$B_{j_1,j_2} = \{\beta_{j_1}\beta_{j_2}(\beta_{j_1} + \beta_{j_2})\}^{2^{m-2}}.$$

For $m = 5$ and 6, by taking α^{j-1} for β_j and the dual basis of $\{1, \alpha, \ldots, \alpha^{m-1}\}$ for $\{\gamma_1^{(m)}, \gamma_2^{(m)}, \ldots, \gamma_m^{(m)}\}$, the following $f^{(2)}_{\ell,h}$ with $1 \leq h \leq m$ are derived:

(1) For $m = 5$,

$$\begin{aligned}
f^{(2)}_{7,1} &= x_2x_3 \oplus x_2x_4 \oplus x_3x_5, \\
f^{(2)}_{7,2} &= x_1x_3 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3 \oplus x_3x_5, \\
f^{(2)}_{7,3} &= x_1x_4 \oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_5 \oplus x_4x_5, \\
f^{(2)}_{7,4} &= x_1x_2 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_4x_5, \\
f^{(2)}_{7,5} &= x_1x_4 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_4 \oplus x_4x_5.
\end{aligned}$$

(2) For $m = 6$,

$$\begin{aligned}
f^{(2)}_{15,1} &= x_2x_3 \oplus x_2x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_6, \\
f^{(2)}_{15,2} &= x_1x_2 \oplus x_1x_4 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_4 \oplus x_4x_5 \oplus x_5x_6, \\
f^{(2)}_{15,3} &= x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_6 \oplus x_3x_4 \oplus x_4x_6, \\
f^{(2)}_{15,4} &= x_1x_4 \oplus x_1x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_6 \oplus x_5x_6, \\
f^{(2)}_{15,5} &= x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_5 \oplus x_1x_6 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_6 \oplus x_4x_6, \\
f^{(2)}_{15,6} &= x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_6 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_6 \oplus x_5x_6.
\end{aligned}$$

$\Delta\Delta$

Let $a(\neq 0)$ and b be elements of GF(2^m). For $0 \leq i < 2^m$, let $\pi_{a,b}(i)$ be a permutation on $\{0, 1, 2, \ldots, 2^m - 1\}$ defined as follows:

(1) For $i = 0$, if $b = 0$, then $\pi_{a,b}(0) = 0$, and otherwise, $\pi_{a,b}(0) = j$ where $\alpha^j = b$.

(2) For $i \neq 0$, if $a\alpha^{i-1}+b = 0$, then $\pi_{a,b}(i) = 0$, and otherwise, $\pi_{a,b}(i) = j$ where $\alpha^j = a\alpha^{i-1}+b$.

This permutation is called an affine permutation. The extended codes of primitive BCH codes, cyclic Reed-Muller codes and some other cyclic codes are known to be invariant under the affine permutations [5]. The following lemma is used in the next section.

Lemma 4: Suppose that the extended code ex-C of a binary linear code C is invariant under the affine permutations. For a boolean polynomial $f(x_1, x_2, \ldots, x_m)$ and a binary m-tuple $\bar{b} = (b_1, b_2, \ldots, b_m)$, let $f_{\bar{b}}(x_1, x_2, \ldots, x_m)$ be defined as

$$f_{\bar{b}}(x_1, x_2, \ldots, x_m) = f(x_1 \oplus b_1, x_2 \oplus b_2, \ldots, x_m \oplus b_m). \tag{3.29}$$

If f represents a codeword of ex-C, then for any binary m-tuple $\bar{b}$, $f_{\bar{b}}$ also represents a codeword of ex-C.

Proof: Let b be defined as

$$b = \sum_{j=1}^{m} b_j \beta_j. \tag{3.30}$$

then it follows from (3.1), (3.2) and the definition of $\pi_{1,b}$ that for $0 \leq i < 2^m$,

$$\begin{aligned} f_{\bar{b}}(a_{i1}, a_{i2}, \ldots, a_{im}) &= f(a_{i1} \oplus b_1, a_{i2} \oplus b_2, \ldots, a_{im} \oplus b_m) & (3.31) \\ &= f(a_{i'1}, a_{i'2}, \ldots, a_{i'm}), & (3.32) \end{aligned}$$

where $i' = \pi_{1,b}(i)$. That is,

$$C(f_{\bar{b}}) = \pi_{1,b} C(f). \tag{3.33}$$

$\Delta\Delta$

4. Application of boolean polynomial representation to construction of trellis diagrams of binary linear codes

In this section, we apply boolean polynomial representation of a linear block code to construct its trellis diagram. In particular, we focus on the construction of minimal trellises for (non-cyclic) reed-Muller codes and the extended and permuted primitive BCH codes which contain Reed-Muller codes as subcodes.

For a positive integer m and a nonnegative integer r not greater than m, let $P^r[x_1, x_2, \ldots, x_m]$ (or P_m^r) denote the set of all boolean polynomials of degree r or less with m variables $x_1, x_2, \ldots, x_m$. For a nonnegative integer i less then 2^m, let $(b_{i1}, b_{i2}, \ldots, b_{im})$ be the standard binary expression of i such that $i = \sum_{j=1}^{m} b_{ij} 2^{m-j}$. For a binary 2^m-tuple $\mathbf{v} = (v_0, v_1, \ldots, v_{2^m-1})$, a boolean polynomial $f(x_1, x_2, \ldots, x_m)$ is said to represent $\mathbf{v}$ with respect to the standard binary order of bit positions if and only if

$$v_i = f(b_{i1}, b_{i2}, \cdots, b_{im}), \text{ for } 0 \leq i < 2^m. \tag{4.1}$$

In this case, $\mathbf{v}$ is denoted $b(f)$. For a binary code C of length 2^m, let $\mathbf{P}[C]$ denote the set of boolean polynomials with variables $x_1, x_2, \ldots, x_m$ such that

$$C = \{b(f) : f \in \mathbf{P}[C]\}. \tag{4.2}$$

For $0 \leq r \leq m$, the r-th order (noncyclic) Reed-Muller code of length 2^m [5, 7], denoted $\mathrm{RM}_{m,r}$, is defined as $\{b(f) : f \in P_m^r\}$, this is, $\mathbf{P}[\mathrm{RM}_{m,r}] = P_m^r$.

Let π_c denote the permutation on $\{0, 1, 2, \ldots, 2^m - 1\}$ such that for $0 \leq i < 2^m$,

$$\pi_c(i) \triangleq \sum_{j=1}^{m} a_{ij} 2^{m-j}, \tag{4.3}$$

where $a_{i1}, a_{i2}, \ldots, a_{im}$ are defined by (3.1). Then π_c is a permutation from a cyclic order to the standard order of bit positions. It follows from (3.1) and (4.1) that for a boolean polynomial f with m variables,

$$\pi_c(f) = b(f). \tag{4.4}$$

Suppose we apply π_c to permute the bit positions of ex-$\mathrm{BCH}_{m,2^{m-r}-1}$ and $(\text{ex-}\mathrm{BCH}_{m,q(m,r)})^{\perp}$. The we have

$$\pi_c[\text{ex-}\mathrm{BCH}_{m,2^{m-r}-1}] \supseteq \mathrm{RM}_{m,r}, \quad \text{for } 1 \leq r < m, \tag{4.5}$$

$$\pi_c[(\text{ex-}\mathrm{BCH}_{m,q(m,r)})^{\perp}] \supseteq \mathrm{RM}_{m,r}, \tag{4.6}$$

for $q(m,1) = 5$ and $q(m,2) = 2^{\lfloor m/2 \rfloor} + 3$.

For a binary code C of length 2^m, C is said to be s-invariant, if and only if for any binary m-tuple $\bar{a}$,

$$b(f_{\bar{a}}) \in C \iff b(f) \in C \tag{4.7}$$

where $f_{\bar{a}}$ is defined by (3.29).

Let A be an invertible affine transformation over binary m-tuples:

$$y_i = c_{i0} \oplus \sum_{j=1}^{m} c_{ij} x_j, \qquad \text{for } 1 \le i \le m. \tag{4.8}$$

For a binary code C of length 2^m which is specified by the set $\mathbf{P}[C]$ of boolean polynomials, let $\pi_A[C]$ be defined as

$$\pi_A[C] \triangleq \left\{ b(f(c_{10} \oplus \sum_{j=1}^{m} c_{1j} x_j, c_{20} \oplus \sum_{j=1}^{m} c_{2j} x_j, \right.$$
$$\left. \ldots, c_{m0} \oplus \sum_{j=1}^{m} c_{mj} x_j)) \quad : \quad f \in \mathbf{P}[C] \right\}. \tag{4.9}$$

Since $\pi_A[\mathrm{RM}_{m,r}] = \mathrm{RM}_{m,r}$ for any affine invertible transformation A over binary m-tuples, it follows from (4.5) and (4.6) that for $1 \le r < m$,

$$\pi_A[\pi_c[\text{ex-BCH}_{m,2^{m-r}-1}]] \supseteq \mathrm{RM}_{m,r}, \tag{4.10}$$

$$\pi_A[\pi_c[(\text{ex-BCH}_{m,q(m,r)})^{\perp}]] \supseteq \mathrm{RM}_{m,r}. \tag{4.11}$$

If a binary code C of length 2^m is invariant under the affine permutations, then it follows from Lemma 4 that $\pi_A[\pi_c[C]]$ is s-invariant. For example, $\pi_A[\pi_c[\text{ex-BCH}_{m,d}]]$ and $\mathrm{RM}_{m,r}$ are s-invariant.

For a nonnegative integer r not greater than m and two integers h and h' such that $0 \le h < h' \le 2^m$, let $P^r_{h,h'}[x_1, x_2, \ldots, x_m]$ (or $P^r_{m,h,h'}$) be defined as follows:

$$P^r_{h,h'}[x_1, x_2, \ldots, x_m] \triangleq \{f \in P^r[x_1, x_2, \ldots, x_m] :$$
$$f(b_{j_1}, b_{j_2}, \ldots, b_{j_m}) = 0 \text{ for } 0 \le j < h \text{ or } h' \le j < 2^m\}. \tag{4.12}$$

For a binary linear code C of length 2^m, it follows from (4.12) that for $f \in \mathbf{P}[C] \cap P^r_m$, $b(f) \in C_{h,h'}$ if and only if

$$f \in P^r_{m,h,h'},$$

where $C_{h,h'}$ is defined in Section 2.

Let $\bar{x}_i$ denote $1 \oplus x_i$. From the definition of (4.12) it holds that

$$f(x_1, x_2, \ldots, x_m) \in P^r_{2^m-h',2^m-h}[x_1, x_2, \ldots, x_m]$$

if and only if

$$f(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m) \in P^r_{h,h'}[x_1, x_2, \ldots, x_m]. \tag{4.13}$$

Now we have Theorem 3.

Theorem 3: Suppose that C is an s-invariant linear binary code of length 2^m. Then the following symmetry holds:

(1) The minimal trellis diagram for C is invariant under reversing the direction of every branch, and (2)

$$K_{h,h'} = K_{2^m-h',2^m-h}, \quad \text{for } 0 \le h < h' \le 2^m, \tag{4.14}$$

$$K_h = K_{2^m-h}, \quad \text{for } 0 \le h \le 2^m. \tag{4.15}$$

Proof:

(1) It follows from the definition (4.7) that for $f(x_1, x_2, \ldots, x_m) \in \mathbf{P}[C]$, $f(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_m) \in \mathbf{P}[C]$. Note that for $(v_0, v_1, \ldots, v_{2^m-1}) = b(f) \in C$, $(v_{2^m-1}, v_{2^m-2}, \ldots, v_0) = b(f(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_m)) \in C$. Then we readily see that the symmetry (1) holds.

(2) Equation (4.14) follows from (4.13) and (4.7), and equation (4.15) follows from (2.9) and (4.14).

ΔΔ

Next we show how to find $K_{h,h'}$ for a binary linear code which contains a Reed-Muller code as a large subcode.

A polynomial $f \in P^r[x_1, x_2, \ldots, x_m]$ is expressed uniquely as the following form:

$$f = a_0 \oplus \sum_{t=1}^{r} \sum_{1 \le j_1 < j_2 < \cdots < j_t \le m} a_{j_1 j_2 \ldots j_t} x_{j_1} x_{j_2} \ldots x_{j_t}, \tag{4.16}$$

where a_0 and $a_{j_1 j_2 \ldots j_t}$ are either 0 or 1. Let ℓ be a positive integer not greater than m. By rearranging the terms in (4.16) with respect to the smallest suffix of variables in a term, f can be uniquely expressed as

$$f = f_{0,\ell} \oplus \sum_{j=1}^{\ell} x_j f_j, \tag{4.17}$$

where $f_j \in P^{r-1}[x_{j+1}, x_{j+2}, \ldots, x_m]$ for $j < m$, $f_m \in \{0, 1\}$, $f_{0,\ell} \in P^r[x_{\ell+1}, x_{\ell+2}, \ldots, x_m]$ for $\ell < m$ and $f_{0,m} \in \{0, 1\}$.

In the following, we will present a necessary and sufficient condition for a polynomial $f \in P_m^r$ to be in $f \in P_{m,h,2^m}^r$. For a positive integer h less than 2^m, suppose that the standard binary expression of $h-1$ is $\sum_{j=1}^{m} b_j 2^{m-j}$. Let the binary sequence $b_1 b_2 \ldots b_m$ be represented as

$$b_1 b_2 \ldots b_m = 0^{\ell_1} 1^{n_1} 0^{\ell_2} 1^{n_2} \cdots 0^{\ell_\tau} 1^{n_\tau},$$

where $0 \le \ell_1 \le m$, $1 \le \ell_t \le m$ for $2 \le t \le \tau$, $1 \le n_t \le m$ for $1 \le t < \tau$, and $0 \le n_\tau \le m$. Let r be a positive integer not greater than m. Define τ' as follows:

(1) If $\tau = 1$ or $\sum_{s=1}^{\tau-1} n_s < r$, then $\tau' \triangleq \tau$.

(2) If $n_1 \ge r$, then $\tau' \triangleq 1$, and otherwise, let τ' denote the greatest integer such that $\sum_{s=1}^{\tau'-1} n_s < r$.

For $1 \le t \le \tau'$, define j_t as $j_1 \triangleq 0$ and $j_t \triangleq \sum_{s=1}^{t-1}(\ell_s + n_s)$. Then the following lemma holds.

Lemma 5: For $f \in P^r[x_1, x_2, \ldots, x_m]$, f is in $P_{h,2^m}^r[x_1, x_2, \ldots, x_m]$ if and only if f can be represented in the following form:

$$f \triangleq f^{(1)}, \tag{4.18}$$

$$f^{(t)} \triangleq g_t \oplus \left(\prod_{j=j_t+\ell_t+1}^{j_t+\ell_t+n_t} x_j \right) f^{(t+1)}, \qquad \text{for } 1 \le t < \tau', \tag{4.19}$$

$$f^{(\tau')} \triangleq g_{\tau'}, \tag{4.20}$$

$$g_1 \triangleq 0, \qquad \text{if } \ell_1 = 0, \tag{4.21}$$

$$g_t \triangleq \sum_{j=j_t+1}^{j_t+\ell_t} x_j g_{t,j}, \qquad \text{if either } \ell_1 \ne 0 \text{ and } t = 1 \text{ and } 1 < t \le \tau', \tag{4.22}$$

where $g_{1,j} \in P^{r-1}[x_{j+1}, x_{j+2}, \ldots, x_m]$ and $g_{t,j} \in P^{r-1-\sum_{s=1}^{t-1} n_s}[x_{j+1}, x_{j+2}, \ldots, x_m]$ for $1 < t \le \tau'$. The above representation is unique if it exists.

Proof: A proof is given in Appendix B. $\Delta\Delta$

Note that equations (4.18) to (4.22) don't depend on τ but depend on τ'. Then we have the following corollary.

Corollary 1: In Lemma 5, consider the case where $\tau > 1$ and $\sum_{s=1}^{\tau-1} n_s \ge r$. Let the binary sequence $b_1' b_2' \cdots b_m'$ and positive integer h' be defined as

$$b_1' b_2' \cdots b_m' \triangleq 0^{\ell_1} 1^{n_1} 0^{\ell_2} 1^{n_2} \cdots 0^{\ell_{\tau'}} 1^{n_{\tau'}'}, \tag{4.23}$$

$$h' - 1 \triangleq \sum_{j=1}^{m} b'_j 2^{m-j}, \tag{4.24}$$

where $n'_{\tau'} \triangleq m - \sum_{s=1}^{\tau'-1} (\ell_s + n_s) - \ell_{\tau'}$. Then it holds that

$$P^r_{h,2^m}[x_1, x_2, \ldots, x_m] = P^r_{h',2^m}[x_1, x_2, \ldots, x_m]. \tag{4.25}$$

$\Delta\Delta$

Example 5: We apply Lemma 5 to the following cases:

(1) Let $h \triangleq 2^{m-u}$ with $0 < u \leq m$. Then $b_1 b_2 \ldots b_m = 0^u 1^{m-u}$, $\ell_1 = u$, $n_1 = m - u$ and $\tau = \tau' = 1$. It follows from Lemma 5 that

$$P^r_{2^{m-u},2^m} = \{x_1 g_1 \oplus x_2 g_2 \oplus \cdots \oplus x_u g_u : g_j \in P^{r-1}[x_{j+1}, \ldots, x_m], \text{ for } 1 \leq j \leq u\}. \tag{4.26}$$

(2) Let $h \triangleq 2^m - 2^{m-u}$ with $0 < u \leq m$. Then, $b_1 b_2 \ldots b_m = 1^{u-1} 0 1^{m-u}$, $\ell_1 = 0$, $n_1 = u - 1$, $\ell_2 = 1$, $n_2 = m - u$ and $\tau = 2$. If $u - 1 < r$ then $\tau' = 2$, and otherwise $\tau' = 1$. It follows from Lemma 5 that

$$P^r_{2^m - 2^{m-u},2^m} = \{x_1 x_2 \ldots x_u g : g \in P^{r-u}[x_{u+1}, \ldots, x_m]\}, \quad \text{for } u \leq r, \tag{4.27}$$

$$= \{0\}, \quad \text{for } u > r. \tag{4.28}$$

(3) Next consider the case where $h = 2^{m-2} + 2^{m-3}$ with $m > 3$. Then $b_1 b_2 \ldots b_m = 0101^{m-3}$, $\ell_1 = n_1 = \ell_2 = 1$, $n_2 = m - 3$ and $\tau = 2$. If $r = 1$, then $\tau' = 1$, and otherwise $\tau' = 2$. From Lemma 5, we have that

$$P^r_{2^{m-2}+2^{m-3},2^m} = \{x_1 g_1 \oplus x_2 x_3 g_2 : g_1 \in P^{r-1}[x_2, \ldots, x_m], g_2 \in P^{r-2}[x_4, \ldots, x_m]\}, \text{for } r \geq 2, \tag{4.29}$$

$$= \{x_1 g_1 : g_1 \in P^{r-1}[x_2, \ldots, x_m]\}, \text{for } r = 1. \tag{4.30}$$

(4) Now consider the case where $h = 2^m - 2^{m-2} - 2^{m-3}$ with $m > 3$. Then $b_1 b_2 \ldots b_m = 10^2 1^{m-3}$, $\ell_1 = 0$, $n_1 = 1$, $\ell_2 = 2$, $n_2 = m - 3$ and $\tau = 2$. If $r = 1$, then $\tau' = 1$, and otherwise $\tau' = 2$. From Lemma 5, we have that

$$P^r_{2^m - 2^{m-2} - 2^{m-3},2^m} = \{x_1(x_2 g_2 \oplus x_3 g_3) : g_2 \in P^{r-2}[x_3, \ldots, x_m], g_3 \in P^{r-2}[x_4, \ldots, x_m]\}, \text{ for } r \geq 2, \tag{4.31}$$

$$= \{0\}, \text{ for } r = 1, \tag{4.32}$$

$\Delta\Delta$

Lemma 6: (1) For $0 < u < m$, let i be a nonnegative integer less than 2^u whose binary expression is $\sum_{j=1}^{u} a_j 2^{u-j}$, and let r be a nonnegative integer not greater than m. If $r < u$, then

$$P^r_{i2^{m-u},(i+1)2^{m-u}}[x_1, x_2, \ldots, x_m] = \{0\}, \tag{4.33}$$

and otherwise it is given by

$$P^r_{i2^{m-u},(i+1)2^{m-u}}[x_1, x_2, \ldots, , x_m] = \{(\prod_{j=1}^{u}(\bar{x}_j \oplus a_j))g : g \in P^{r-u}[x_{u+1}, \ldots, x_m]\}. \tag{4.34}$$

(2) If C is an s-invariant linear binary code of length 2^m, then

$$K_{i2^{m-u},(i+1)2^{m-u}} = K_{0,2^{m-u}}, \tag{4.35}$$

$$K_{\overline{i2^{m-u},(i+1)2^{m-u}}} = K_{2^{m-u},2^m}. \tag{4.36}$$

Proof: (1) Note that $f(x_1, x_2 \ldots, x_m) \in P^r_{i2^{m-u},(i+1)2^{m-u}}[x_1, x_2, \ldots, , x_m]$ if and only if $f(\bar{x}_1 \oplus a_1, \bar{x}_2 \oplus a_2, \ldots, \bar{x}_u \oplus a_u, x_{u+1}, \ldots, x_m) \in P^r_{2^m - 2^{m-u},2^m}[x_1, x_2, \ldots, x_m]$. Then the first part of the lemma follows from (4.27) and (4.28).

(2) Equation (4.35) follows from the above proof (1) and (4.7). If and only if $f(x_1, x_2, \cdots, x_m) \in P^m_{\overline{i2^{m-u},(i+1)2^{m-u}}}[x_1, x_2, \cdots, x_m]$, then

$$f(x_1 \oplus a_1, x_2 \oplus a_2, \cdots, x_u \oplus a_u, x_{u+1}, \cdots, x_m) \in P^m_{\overline{0,2^{m-u}}}[x_1, x_2, \cdots, x_m]. \tag{4.37}$$

Hence, $K_{\overline{i2^{m-u},(i+1)2^{m-u}}} = K_{\overline{0,2^{m-u}}}$. Then equation (4.36) follows from (2.6). $\Delta\Delta$

Structural analysis of trellises for Reed-Muller codes

In the following, we analyze the state and branch complexities of minimal trellis diagrams for Reed-Muller codes and some extended and permuted primitive BCH codes which contain Reed-Muller codes as subcodes.

Let C be the r-th order Reed-Muller code $\mathrm{RM}_{m,r}$ of length $n = 2^m$ with $1 \leq r < m$. For nonnegative integers i and q, let $M(i,q)$ be defined as

$$M(i,q) \triangleq \sum_{j=0}^{\min\{i,q\}} \binom{q}{j}, \tag{4.38}$$

and if i or q is a negative integer, $M(i,q)$ is defined to be zero. By definition,

$$|P^i_q| = M(i,q). \tag{4.39}$$

For $1 \leq h < 2^m$, consider $K_{h,2^m,\mathrm{RM}_{m,r}}$ $(= |P^r_{m,h,2^m}|)$. We use the same notations as those in Lemma 5. The number of polynomials g_t's with $1 \leq t \leq \tau'$ in Lemma 5 is given by

$$\sum_{j=1}^{\ell_t} M(r-1-\textstyle\sum_{s=1}^{t-1} n_s, m-j_t-j),$$

where $\sum_{s=1}^{t-1} n_s = 0$ for $t = 1$, and therefore $K_{h,2^m,\mathrm{RM}_{m,r}}$ is given by

$$K_{h,2^m,RM_{m,r}} = \sum_{t=1}^{\tau'} \sum_{j=1}^{\ell_t} M(r-1-\textstyle\sum_{s=1}^{t-1} n_s, m-j_k-j). \tag{4.40}$$

As special cases, we have that for $0 < u \leq m$,

$$K_{2^{m-u},2^m} = \sum_{j=1}^{u} M(r-1, m-j), \tag{4.41}$$

$$K_{2^m-2^{m-u},2^m} = M(r-u, m-u), \tag{4.42}$$

$$K_{2^{m-2}+2^{m-3},2^m} = M(r-1, m-1) + M(r-2, m-3), \quad \text{for } m \geq 3, \tag{4.43}$$

$$K_{2^m-2^{m-2}-2^{m-3},2^m} = M(r-2, m-2) + M(r-2, m-3), \quad \text{for } m \geq 3. \tag{4.44}$$

From Lemma 6 and (4.39), we see that

$$K_{i2^{m-u},(i+1)2^{m-u}} = M(r-u, m-u), \quad \text{for } 0 \leq i < 2^u. \tag{4.45}$$

It follows from (2.9), (4.14), (4.41), and (4.42) that

$$K_{2^{m-u}} = M(r,m) - M(r-u, m-u) - \sum_{j=1}^{u} M(r-1, m-j). \tag{4.46}$$

Since $M(r,m) = M(r, m-1) + M(r-1, m-1)$, we have that

$$\begin{aligned} K_{2^{m-u}} &= M(r, m-u) - M(r-u, m-u) \\ &= \sum_{j=\max\{0,r-u+1\}}^{\min\{m-u,r\}} \binom{m-u}{j}. \end{aligned} \tag{4.47}$$

Equations (2.11) and (4.47) give the state complexity (number of states) of the minimal trellis diagram for $\mathrm{RM}_{m,r}$ just after the 2^{m-u}-th bit position for $0 < u \leq m$. For examples, it follows from (4.15) and (4.47) that

$$K_{2^{m-1}} = K_{2^{m-2}} = K_{2^m-2^{m-2}} = \binom{m-1}{r}. \tag{4.48}$$

Forney [3] first showed a 4-section trellis diagram with $2^{\binom{m-1}{r}}$ states for $\mathrm{RM}_{m,r}$. In fact, this number is the minimum as shown by (4.48). It follows from (2.9), (4.14), (4.15), (4.43), and (4.44), that

$$\begin{aligned} K_{2^{m-2}+2^{m-3}} &= K_{2^m-2^{m-2}-2^{m-3}} \\ &= M(r,m) - M(r-1,m-1) - M(r-2,m-2) - 2M(r-2,m-3) \\ &= M(r,m-1) - M(r-2,m-2) - 2M(r-2,m-3). \end{aligned} \tag{4.49}$$

Formula (4.49) together with (4.48) gives the minimum number of states at the end of each section of an 8-section trellis diagram for $\mathrm{RM}_{m,r}$ with the same section length.

Now we consider the minimal 2^u-section trellis diagram for $\mathrm{RM}_{m,r}$. From Lemma 6 we see that the subtrellis diagram from a state at the beginning of a section to another state at the end of the section is either empty or can be constructed to be isomorphic to any of trellis diagrams for $\mathrm{RM}_{m-u,r-u}$, where $\mathrm{RM}_{m-u,r-u} = \{\bar{0}\}$, for $r < u$. From (4.14), we have that

$$K_{0,(i+1)2^{m-u}} - K_{0,i2^{m-u}} = K_{2^m-(i+1)2^{m-u},2^m} - K_{2^m-i2^{m-u},2^m}. \tag{4.50}$$

The right-hand side of above equation can be computed by using Lemma 5. For instance, consider the case where $u = 2$. From (4.41) to (4.45) we have that

$$\begin{aligned} K_{0,2^{m-1}} - K_{0,2^{m-2}} &= M(r-1,m-1) - M(r-2,m-2) \\ &= M(r-1,m-2), \end{aligned} \tag{4.51}$$

$$\begin{aligned} K_{0,2^{m-1}+2^{m-2}} - K_{0,2^{m-1}} &= M(r-1,m-1) + M(r-1,m-2) - M(r-1,m-1) \\ &= M(r-1,m-2). \end{aligned} \tag{4.52}$$

From (4.45), (4.51) and (4.52), we have that

$$K_{0,2^{m-2},2^{m-1}} = K_{0,2^{m-1},2^{m-1}+2^{m-2}} = \binom{m-2}{r-1}, \tag{4.53}$$

where $\binom{q}{i} \triangleq 0$ for $q < i$.

Consider the special case where $r = 1$. From Corollary 1 and (4.41) we see that for $0 \le u < m$ and $2^{m-u-1} < h \le 2^{m-u}$,

$$K_{h,2^m} = K_{2^{m-u},2^m} = u. \tag{4.54}$$

It follows from (2.9), (4.14), (4.15) and (4.54) that for $1 \leq u < m$, $2^{m-u-1} < h \leq 2^{m-u}$ and $h \neq 2^{m-1}$, we have

$$K_h = K_{2^m-h} = m - u + 1, \tag{4.55}$$

and

$$K_{2^{m-1}} = m - 1. \tag{4.56}$$

Structural complexity of trellis diagrams for some extended and permuted primitive BCH codes

In the next three examples, we analyze the state and branch complexities of minimal trellis diagrams for some extended and permuted primitive BCH codes of moderate length.

Example 6: Consider ex-$\mathrm{BCH}_{6,15}$, the extended $(64, 24)$ code of the primitive (63,24) BCH code with minimum distance 15 (refer to Example 2). The permuted code $\pi_c[\text{ex-BCH}_{6,15}]$ contains $\mathrm{RM}_{6,2}$, the 2nd-order noncyclic Reed-Muller code of length 64 and minimum distance 16, as a subcode. Then the set of coset leaders of $\pi_c[\text{ex-BCH}_{6,15}]$ /$\mathrm{RM}_{6,2}$ is generated by $b(f^{(3)}_{21,1})$ and $b(f^{(3)}_{21,2})$, where $f^{(3)}_{21,1}$ and $f^{(3)}_{21,2}$ are defined by (3.19) and (3.20) respectively. From Lemma 5 we see that the first 22 components of $b(f^{(3)}_{21,1})$ and the first 21 components of $b(f^{(3)}_{21,2})$ are all zero. Since $\pi_c[\text{ex-BCH}_{6,15}]$ is s-invariant, the symmetry stated in Theorem 3 and equations (4.33) to (4.36) hold. By using (3.19), (3.20) and (4.26) to (4.34), we can find $K_{0,4i,64}$ $(= K_{4i})$, $K_{0,4(i-1),4i}$ and $K_{4(i-1),4i}$ for $1 \leq i \leq 16$ (see Table 1). A 16-section trellis diagram for $\pi_c[\text{ex-BCH}_{6,15}]$ has the following state and branch complexities: For $1 \leq i \leq 16$,

(1) the number of the states at the end of the i-th section (or just after the $4i$-th bit) is $2^{K_{4i}}$; and

(2) for each state s at the $4i$-th bit, there are $2^{K_{0,4(i-1),4i}}$ states at the $4(i-1)$-th bit from which there are branches to s, and the number of parallel branches is $2^{K_{4(i-1),4i}}$. $\Delta\Delta$

Example 7: Consider ex-$\mathrm{BCH}_{6,7}$, the extended (64, 45) code of the primitive (63, 45) BCH code with minimum distance 7 (refer to Example 3). The permuted code $\pi_c[\text{ex-BCH}_{6,7}]$ contains $\mathrm{RM}_{6,3}$, the 3rd-order Reed-Muller code of length 64 and minimum distance 8 as a subcode. The coset leaders of $\pi_c[\text{ex-BCH}_{6,7}]/\mathrm{RM}_{6,3}$ are generated by $b(f^{(4)}_{9,1})$, $b(f^{(4)}_{9,2})$ and $b(f^{(4)}_{9,3})$, where $f^{(4)}_{9,1}$, $f^{(4)}_{9,2}$ and $f^{(4)}_{9,3}$ are defined by (3.26) to (3.28) respectively. The first 27 components of $b(f^{(4)}_{9,1})$, the first 29 components of $b(f^{(4)}_{9,2})$ and the first 30 components of $b(f^{(4)}_{9,3})$

are all zero. In Table 2, $K_{0,4i,64}$ $(= K_{4i})$, $K_{0,4(i-1),4i}$ and $K_{4(i-1),4i}$ for $1 \leq i \leq 16$ are shown. These numbers give the state and branch complexities of the minimal 16-section trellis diagram for π_c[ex-BCH$_{6,7}$]. $\Delta\Delta$

Example 8: Let C be ex-BCH$_{m,5}$, the extended code of the primitive binary BCH code of length $2^m - 1$ and minimum distance 5 with $m \geq 3$. The dual code of C, $C^\perp$, is the extended code of the dual code of the even weight subcode of the BCH$_{m,5}$, and $\pi_c[C^\perp]$ contains RM$_{m,1}$ as a subcode. Let C' denote the subcode $\pi_c[C^\perp] - \text{RM}_{m,1}$ of $\pi_c[C^\perp]$. The dimension of C' is m. Consider the minimal 4-section trellis diagram T_4 for $\pi_c[C]$. Then it follows from Lemma 3, (2.27), (4.55) and (4.56) that the state complexity of T_4 is about 1/4 of that of the minimal 4-section trellis diagram for C.

For a boolean polynomial f with m variables, a linear subspace U of the set of binary m tuples which are generated by $\bar{u}_i = (u_{i1}, u_{i2}, \ldots, u_{im})$ with $1 \leq i \leq h$ is said to be a maximal Z-space of f if and only if U is a maximal linear subspace with the following property:

> There are binary constants $u_{10}, u_{20}, \ldots, u_{h0}$ such that for every binary tuple $(b_1, b_2, \ldots, b_m)$ in $\{(b_1, b_2, \ldots, b_m) \ : \ \sum_{i=1}^{m} u_{ij} b_j = u_{i0} \quad \text{for } 1 \leq i \leq h\}$,
>
> $$f(b_1, b_2, \ldots, b_m) = 0.$$

We found the set of maximal Z-spaces for each polynomial in $\mathbf{P}(C')$. By using this knowledge, we chose the following affine invertible transformation A to make $K_{0,2^{m-2},\pi_A[\pi_c[C^\perp]]}$ and $K_{0,2^{m-2}+2^{m-3},\pi_A[\pi_c[C^\perp]]}$ as small as possible. For $m = 5$, let A be the invertible linear transformation: $y_1 = x_5$, $y_2 = x_4 + x_5$, $y_3 = x_1 + x_2 + x_3 + x_5$, $y_4 = x_3$ and $y_5 = x_2$. Then from Example 4 we see that the coset leaders of $\pi_A[\pi_c[C^\perp]]/\text{RM}_{5,1}$ are generated by $b(f_i)$ with $1 \leq i \leq 5$ where f_i is defined as follows:

$$\begin{aligned}
f_1 &\triangleq y_1 y_4 + (y_1 + y_2 + y_4) y_5, \\
f_2 &\triangleq (y_1 + y_3 + y_4 + y_5) y_2 + y_3 y_4, \\
f_3 &\triangleq y_1 y_4 + y_2 (y_3 + y_4), \\
f_4 &\triangleq y_2 y_4 + y_3 y_5, \\
f_5 &\triangleq y_1 (y_3 + y_5) + y_2 y_3.
\end{aligned}$$

By using (2.26), (2.27), (4.35), (4.36), (4.54) to (4.56), we can find $K_{4i,C}$, $K_{0,4(i-1),4i,C}$, and $K_{4(i-1),4i,C}$ for $1 \leq i \leq 8$ which give the state and branch complexities of an 8-section trellis diagram for the code $\pi_A[\pi_c[\text{ex-BCH}_{5,5}]]$ (see Table 3). $\Delta\Delta$

5. Conclusion

In this paper, we have investigated the trellis structure of linear block codes, particularly the state and branch complexities of the minimal trellis diagram of a linear block code. We have shown that a cyclic (or shortened cyclic) code is the worst in terms of the state complexity of its minimal trellis diagram among the linear codes of the same length and dimension. We have considered the boolean polynomial representation of codewords of a cyclic code and applied this representation to construct minimal trellises for codes obtained from cyclic codes by properly permuting their bit positions. Particularly, we have focused on the construction of minimal trellises for extended and permuted primitive BCH codes which contain Reed-Muller codes as subcodes. We have shown that some extended and permuted primitive BCH codes of moderate length have relatively simple trellis diagrams. Good block codes with simple trellises are attractive for error control in digital communications, because they can be practically decoded with soft-decision optimal or suboptimal decoding algorithm. Soft-decision multi-stage suboptimal decoding algorithms for some BCH codes are under study [10]. In construction of multi-level block modulation codes of moderate length with the multi-level method, it is desirable to use good block codes with simple trellises as component codes. This allows us to use multi-stage decoding in which each component code is decoded with the soft-decision Viterbi decoding algorithm [9]. Using the soft-decision multi-stage decoding, it is possible to achieve high spectral efficiency and large coding gain with reduced decoding complexity.

Appendix A

Proof of Theorem 1

For $s \in S_h$ and $s' \in S_{h'}$, let $\sigma(s')$ denote the set of states in S_h from which there is a path to s', and let $\sigma'(s)$ denote the set of states in $S_{h'}$ to which there is a path from s. From (2.9), (2.6) and (2.8), $|p_{0,h}[C]/p_{0,h}[C^{tr}_{0,h'}]| = 2^{K-K_{h,N}-(K_{0,h'}-K_{h,h'})} = 2^{K_{0,h,N}-K_{0,h,h'}} = 2^q$. Partition S_h into 2^q blocks $S_{h1}, S_{h2}, \ldots, S_{h2^q}$ in such a way that states s_1 and s_2 in S_h are in the same block if and only if $\varphi(s_1)$ and $\varphi(s_2)$ are in the same coset of $p_{0,h}[C]/p_{0,h}[C^{tr}_{0,h'}]$. Since each coset of $p_{0,h}[C]/p_{0,h}[C^{tr}_{0,h'}]$ contains exactly $|p_{0,h}[C^{tr}_{0,h'}]/C^{tr}_{0,h}|$ cosets of $p_{0,h}[C]/C^{tr}_{0,h}$, every block S_{hi} has the same size. Lemma 1 implies that for $s' \in S_{h'}$, there is exactly one index i such that

$$\sigma(s') = S_{hi}. \tag{A.1}$$

For $1 \le i \le 2^q$, let $S_{h'i}$ be defined as

$$S_{h'i} \triangleq \{s' \in S_{h'} : \text{for } s \in S_{hi}, \varphi(s) + p_{0,h}\varphi(s') \in p_{0,h}[C^{tr}_{0,h'}]\}.$$

Then it follows from Lemma 1 that for $s \in S_{hi}$,

$$\sigma'(s) = S_{h'i}. \tag{A.2}$$

For each α in $p_{0,h}[C]$, the number of binary sequences β's such that $\alpha \circ \beta \in p_{0,h'}[C]$ is $|C^{tr}_{h,h'}|$ from (2.17). Hence $|S_{h'i}| = |p_{0,h}[C^{tr}_{0,h'}]| \cdot |C^{tr}_{h,h'}|/|C^{tr}_{0,h'}|$, and every block $S_{h'i}$ has the same size.

If $L(s,s')$ is not empty, then it follows from (2.2) and (2.23) that $L(s,s')$ is a coset of $p_{h,h'}[C]/C^{tr}_{h,h'}$ and $|L(s,s')| = 2^{K_{h,h'}}$. $\Delta\Delta$

Appendix B

Proof of Lemma 5

For two binary ℓ-tuples $(a_1, a_2, \ldots, a_\ell)$ and $(a'_1, a'_2, \ldots, a'_\ell)$, we write $(a_1, a_2, \ldots, a_\ell) \leq (a'_1, a'_2, \ldots, a'_\ell)$, if and only if

$$\sum_{i=1}^{\ell} a_i 2^{\ell-i} \leq \sum_{i=1}^{\ell} a'_i 2^{\ell-i}.$$

For every binary m-tuple $(a_1, a_2, \ldots, a_m) \leq (b_1, b_2, \ldots, b_m)$, denoted $\mathbf{b}$,

$$f(a_1, a_2, \ldots, a_m) = 0, \tag{B.1}$$

if and only if $f \in P^r_{h,2^m}[x_1, x_2, \ldots, x_m]$.

We prove this lemma by induction. If $m = 1$, then $h = 1, \tau = 1, \ell_1 = 1$ and $n_1 = 0$. Since $P^r_{1,2}[x_1] = \{0, x_1\}$, this lemma is true. Consider the case where $m \geq 2$.

Suppose that $f \in P^r_{h,2^m}[x_1, x_2, \ldots, x_m]$. If $\ell_1 = m$ and $n_1 = 0$, then let $\ell \triangleq m$ and otherwise, let $\ell \triangleq \ell_1 + 1$. Express f as the form of (4.17). Since it follows form (B.1) that $f(\overbrace{0, 0, \ldots, 0}^{\ell}, x_{\ell+1}, \ldots, x_m) = 0$, $f_{0,\ell}$ must be zero.

(1) If $n_1 = 0$, then $\ell_1 = m$, $h = 1$ and

$$f = \sum_{j=1}^{m} x_j f_j = g_1.$$

Conversely, f of the above form is in $P^r_{2,2^m}[x_1, x_2, \ldots, x_m]$.

(2) If $n_1 > 0$, then

$$f = \sum_{j=1}^{\ell_1 \oplus 1} x_j f_j = g_1 \oplus x_\ell f_\ell.$$

Note that

$$f_\ell = f(\overbrace{0, 0, \ldots, 0, 1}^{\ell}, x_{\ell+1}, \ldots, x_m) \in P^{r-1}[x_{\ell+1}, \ldots, x_m]. \tag{B.2}$$

(2.1) Suppose that $\tau' = 1$. (i) If $\tau = 1$, then for every binary $(m-\ell)$-tuple, $(\overbrace{0, 0, \ldots, 0, 1}^{\ell}, a_{\ell+1}, \ldots, a_m) \leq (\overbrace{0, 0, \ldots, 0, 1}^{\ell}, 1, \ldots, 1) = \mathbf{b}$. From (B.1), $f(\overbrace{0, 0, \ldots, 0, 1}^{\ell}, a_{\ell+1}, \ldots, a_m) = 0$. That is, $f_\ell = 0$. (ii) If $\tau > \tau' = 1$, then $n_1 \geq r$. If $f(\overbrace{0, 0, \ldots, 0, 1}^{\ell}, a_{\ell+1}, \ldots, a_m) = 1$, then it follows from (B.1) that $\mathbf{b} = (\overbrace{0, 0, \ldots, 0}^{\ell_1}, \overbrace{1, 1, \ldots, 1}^{n_1}, b_{\ell_1+n_1+1}, \ldots, b_m) < (0, 0, \ldots, 0, 1, a_{\ell+1}, \ldots, a_m)$. Hence $a_j = 1$ for $\ell + 1 \leq j \leq$

$\ell_1 + n_1$. Consequently, the weight[*3] of $f_\ell \in P^{r-1}[x_{\ell+1}, \ldots, x_m]$ is at most $2^{m-\ell_1-n_1} - 1 < 2^{m-\ell-(r-1)}$, and therefore $f_\ell = 0$. For these two cases, $f = g_1$. Conversely, f of this form is in $P^r_{h,2^m}[x_1, x_2, \ldots, x_m]$.

(2.2) Suppose that $r' > 1$. Then $r \geq 2$ and $r \geq 2$. Let h' denote $1 + \sum_{j=\ell+1}^{m} b_j 2^{m-j}$. Then $1 \leq h' < 2^{m-\ell}$. It follows from (B.2) that $f \in P^r_{h,2^m}[x_1, x_2, \ldots, x_m]$ if and only if

$$f_\ell \in P^{\min(r-1,m-\ell)}_{h',2^{m-\ell}}[x_{\ell+1}, \ldots, x_m],$$

where $1 < \ell + 1 \leq m$. Let $f^{(2)} \triangleq f_\ell$. Then this lemma is proved by induction hypothesis. $\Delta\Delta$

References

[1] J. Wolf, "Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis," *IEEE Trans. on Information Theory*, Vol. IT-24, No. 1, pp. 76–80, January 1978.

[2] G.D. Forney, Jr., et al., "Efficient Modulation for Band-Limited Channels," *IEEE Journal on Selected Areas in Communications*, Vol. SAC-2, No. 5, September 1984.

[3] G.D. Forney, Jr., "Coset Codes—Part II: Binary Lattices and Related Codes," *IEEE Trans. on Information Theory*, Vol. IT-34, No. 5, pp. 1152–1187, September 1988.

[4] J. Snyders and Y. Beery, "Maximum Likelihood Soft Decoding of Binary Block Codes and Decoders for the Golay Codes," *IEEE Trans. on Information Theory*, Vol. IT–35, No. 5, pp. 963–975, September 1989.

[5] W.W. Peterson and E.J. Weldon, Jr., Error-Correcting Codes, MIT Press, 1972.

[6] S. Lin and D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Prentice-Hall, New Jersey, 1983.

[7] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[8] T. Kasami, T. Takata, T. Fujiwara and S. Lin, "On Linear Structure and Phase Rotation Invariant Properties of Block 2^ℓ-PSK Modulation Codes," *IEEE Transactions on Information Theory*, 1990, to be published.

[9] S. Ujita, T. Takata, T. Fujiwara, T. Kasami and S. Lin, "A Multi-stage Decoding for Block Modulation Codes and Its Error Probability Analysis," *the Proceedings of the 12th Symposium on Information Theory and Its Applications*, Inuyama, Japan, December 6–9, 1989.

[*3] The weight of f is defined as the Hamming weight of $b(f)$. It is known that the weight of nonzero f degree r or less with m variables is at least 2^{m-r} [5, 6, 7].

[10] T. Takata, S. Ujita, T. Kasami and S. Lin, "A Multi-stage Decoding for Multi-level Block Modulation Codes and Its Error Probability Analysis," to be presented at *the International Symposium on Information and Its Applications*, Honolulu, HI, November 25–27, 1990.

Table 1

The complexity of a 16-section trellis diagram for π_c[ex-BCH$_{6,15}$], an equivalent code of the extended (64, 24) code of the primitive (63, 24) BCH code

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
K_{4i}	4	7	10	10	13	15	15	12	15	15	13	10	10	7	4	0
$K_{4i,\mathrm{RM}_{6,2}}$	4	7	10	10	13	13	13	10	13	13	13	10	10	7	4	0
$K_{4(i-1),4i}$	0															
$K_{0,4(i-1),4i}$	0	0	0	1	0	1	1	3	0	1	3	3	1	3	3	4
$K_{0,4(i-1),4i,\mathrm{RM}_{6,2}}$	0	0	0	1	0	1	1	3	0	1	1	3	1	3	3	4

(1) The number of states at the end of the i-th section (or just after the $4i$-th bit) is $2^{K_{4i}}$.

(2) For each state s at the $4i$-th bit, there are $2^{K_{0,4(i-1),4i}}$ states at the $4(i-1)$-th bit from which there are branches to s, and the number of parallel branches is $2^{K_{4(i-1),4i}}$.

Table 2

The complexity of a 16-section trellis diagram for π_c[ex-BCH$_{6,7}$], an equivalent code of the extended (64, 45) code of the primitive (63, 45) BCH code

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
K_{4i}	4	7	10	10	13	13	14	13	14	13	13	10	10	7	4	0
$K_{4i,\mathrm{RM}_{6,3}}$	4	7	10	10	13	13	13	10	13	13	13	10	10	7	4	0
$K_{4(i-1),4i}$	0															
$K_{0,4(i-1),4i}$	0	1	1	3	1	3	3	4	3	4	3	4	3	4	4	4
$K_{0,4(i-1),4i,\mathrm{RM}_{6,3}}$	0	1	1	3	1	3	3	4	1	3	3	4	3	4	4	4

Table 3

The complexity of an 8-section trellis diagram for $\pi_A[\pi_c[\text{ex-BCH}_{5,5}]]$, an equivalent code of the extended (32,21) code of the primitive (31,21) BCH code

i	1	2	3	4	5	6	7	8
K_{4i}	4	7	9	9	9	7	4	0
$K_{4i,\text{RM}_{5,1}}$	3	4	5	4	5	4	3	0
$K_{4(i-1),4i}$	0							
$K_{0,4(i-1),4i}$	0	1	2	3	3	4	4	4
$K_{0,4(i-1),4i,\text{RM}_{5,1}}$	0	0	0	1	0	1	1	3

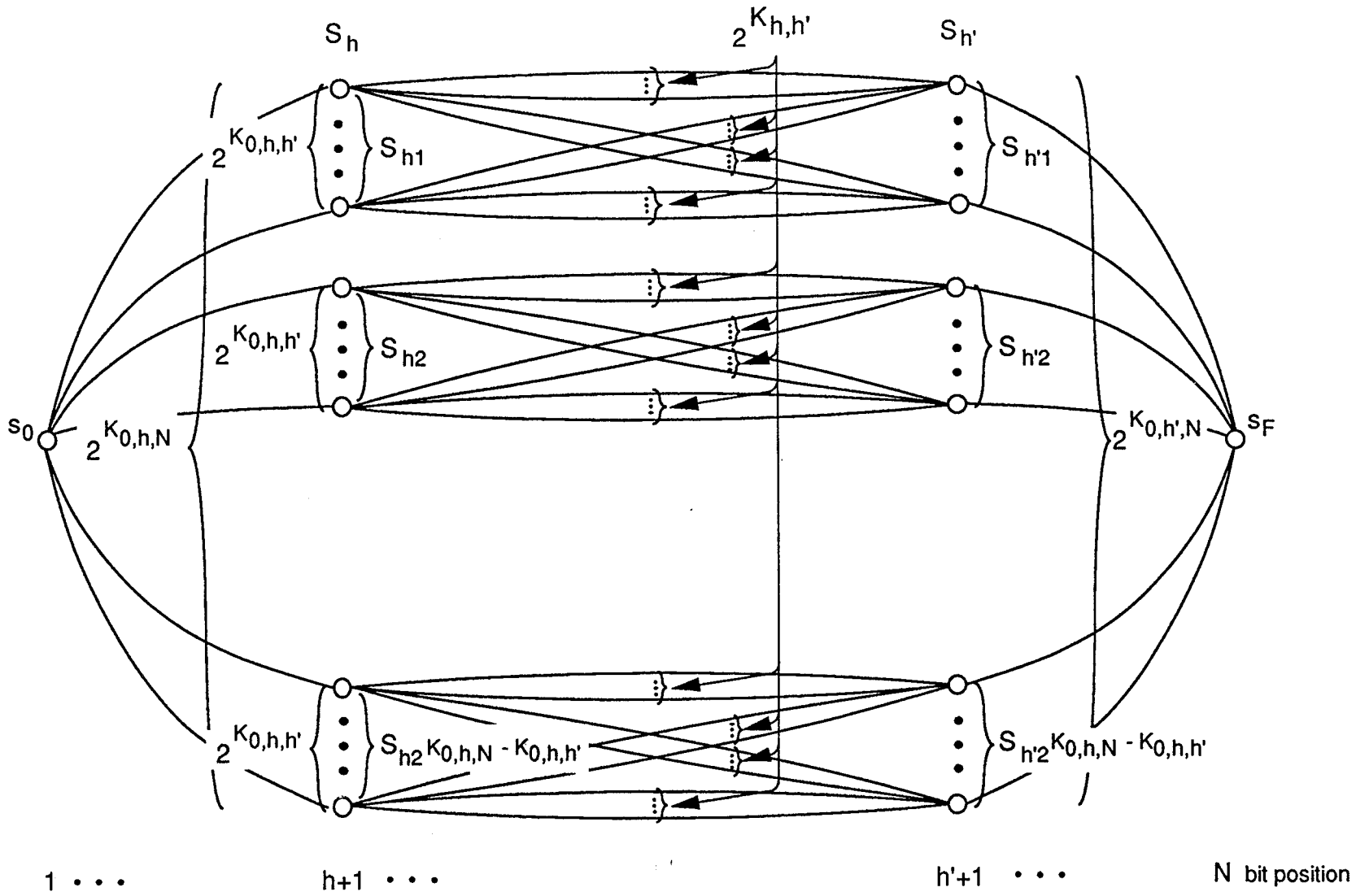

Figure 1 : The branch complexity of a trellis diagram with the minimum number of states